

REMARKS

This Amendment is in response to the Office Action of April 23, 2008 in which claims 1-24 were rejected. New dependent claims 25-32 have been added to cover the subject matter disclosed at page 5, line 29 to page 6, line 5 with the mentioned advantages. Further support may be found at page 11, line 23 to page 12, line 12.

Regarding the subject matter of independent method claim 1, it can be understood by viewing the claim alongside Fig. 2. In Fig. 2, a secure channel 207 is shown connecting a server 208 to an installation part 203 of an application 202 and connecting the installation part 203 to a secure environment 205 in the device 201. The device 201 may be a terminal device as claimed in claim 1 and receive a first key in its secure environment 205 via the secure channel 207 from the server 208 outside the terminal 201. The first key is for decrypting an encrypted application 204. The secure channel 207 may for example (as discussed in the specification) involve the server 208 encrypting the first key with a public key of device 201. It is also possible to for instance use the SSL protocol to transfer the first key into the secure environment 205. See page 3, paragraph 0028 in the right-hand column at lines 14-23. The protected (encrypted) application part 204 is then decrypted in the secure environment 205 by means of the first key (which came from the server). Before being stored back outside the secure environment, the application is re-encrypted in the secure environment by means of a second key.

In Section 5 beginning on page 2 of the Detailed Action, the Examiner refers to *Cassagnol* for disclosing the receiving in a secure environment in a terminal via a secure channel from a server outside the terminal a first key for decrypting an encrypted application, pointing to paragraphs 0109-0112. These paragraphs cover the first two steps shown in Fig. 6 of *Cassagnol*. In those steps, the test jig 122 with the adapter 10 uses the public key of the server 120 to encrypt a triple DES session key which it then sends to the server 120 via the network 128. The key server decrypts the triple key generated in the test jig using its private key so as to access the session key. The key server then sends the apparatus 10 some random numbers

from the key server's source 126 to update the seed material on the apparatus 10. It will also send any assigned configuration, such as a serial number, and a software export/import master key (MK). This is shown in the second arrow in Fig. 6 going from right to left and labeled DES (Config). This is presumably encrypted with the session key received from the test jig 122.

The remaining part of Fig. 6 also has to do with the generation, encryption and reprogramming of the EEPROM 32 of Fig. 3 which is the repository of the key material (see page 8 at paragraph 71 and page 9 at paragraph 0086).

Notice that there is nothing discussed here about decryption or re-encryption of an application part such as the application part 204 of Fig. 2 of the present disclosure. In other words, the statement by the Examiner that the first key is for decrypting an encrypted application does not seem to correspond to what is shown in Figs. 5 and 6 of *Cassagnol* which seem to deal with key management.

The Examiner seems to recognize this fact by reference to paragraph 0025 of *Cassagnol* which the Examiner asserts discloses decrypting, in the secure environment, the encrypted application by means of the first key, pointing to the whitening key disclosed in paragraph 0025. However, this whitening key is not sent by the key server in Fig. 5 or 6 but rather is generated by the adapter 10 itself.

The Examiner goes on to analogize the re-encrypting in the secure environment to this same whitening key.

In a telephone conversation between the undersigned and the Examiner, the undersigned requested the Examiner to clarify exactly what was meant by the first key in the above analysis. The Examiner confirmed that he is referring to the MK key which, as explained above, is shown in the second arrow of Fig. 6 being transferred from the key server 120 to the test jig 122. But the citation at 0025 does not refer to using any such first key to decrypt an encrypted application as claimed in claim 1. So, it seems that the Examiner's analysis is missing this crucial aspect of the claim where it is stated that the encrypted application is decrypted by means of the first key.

In other words, at the most, the Examiner has here only shown the receipt of the first key.

The claimed first key and the software export/import master key MK in paragraph 0112 of *Cassagnol* are not the same. In *Cassagnol* the whitening processes are performed by the cipher means, which comprises a crypto module 20 (see Fig. 3) which is capable of performing triple key encryption and decryption with whitening etc. [0048, 0056]. The encryption/decryption key is employed by the cipher means are protected utilizing a key hierarchy. The triple DES process is keyed with the session key. To obtain the session key one must have the master key, and to obtain the master key access to the device key is required [0061]. Further, in the same paragraph [0061] it is stated that unencrypted versions of the session key, the master key, and the device key are only available in the cipherer 20 and the cipherer's key facility.

Further still, in paragraphs 0110-0112, the communication process between the device and the server as shown in Fig. 6 is described as one in which the device first creates a new random seed which is then used to create a session key. To obtain the session key one must have the master key, and to obtain the master key access to the device key is required. This is all done within the device. In other words, a master key is employed in the device. The session key is then encrypted with the public key of the key server and is sent to the key server, which session key is then decrypted with the private key of the server and utilized for any further communication between the device and the server. Thereafter, an export/import master key (MK) is sent to the test jig.

Still further, in [0085] it is stated that the generation of *whitening keys* is obtained by utilizing an entropy source 408, the CSPRNG and further in [0086] the route key (device key) for the key hierarchy is loaded via the key isolation circuit. (This is shown only as a signal line in Fig. 3.) To ensure the keys cannot be accessed ... the memory 32, the logic circuit 34, the key isolation circuit 50 and the crypto module 20 define a *closed system*.

From the foregoing, it appears that the term master key is used in a very unclear way in the document and it is not clear from the document nor is it explicitly shown how this export/import MK is used.

In fact, it is emphasized in [0104, 0105] that is more secure to generate keys within the device by self-keying. If it can be shown that the export/import master key is indeed used to obtain the first key, being the first whitening key, by the crypto module utilizing the key hierarchy as described above, it is at least true that the export/import MK is not equal to the first key according to the present invention. Thus, the present inventive concept of receiving the first key to decrypt an encrypted application via a secure channel is not shown in *Cassagnol* which, on the contrary, supports self-keying and generation of any keys within the device.

Regarding dependent claim 3, which depends from claim 1, it claims that the first key is encrypted by the second key. Nowhere in the *Cassagnol* document is it explicitly shown that the whitening key is used to encrypt the first key for storage outside the secure environment.

With regard to independent claim 2, it again has not been shown explicitly in the *Cassagnol* reference where the first key that is for decrypting an encrypted application is encrypted by means of a second key and stored outside the secure environment. The passage at paragraph 0058 of *Cassagnol* does not seem to disclose anything like that. It does discuss an encrypted version of the whitening key but that is not the same thing as the first key received from the key server 120.

Regarding claims 8-10 and 22-24, the same comments apply as made above to the extent that they encompass the same scope as claims 1-3.

Withdrawal of the novelty rejection is requested.

Regarding the obviousness rejection recited in Section 10 on page 4, the Examiner refers to the secondary reference *Matyas et al* for showing the missing symmetric second key that can be derived from the application. Claim 4 depends from claim 1 and claims 5 and 6 from claim 4 and these claims are patentably nonobvious for at least the same reasons given above in applicant overcoming the novelty rejection of the independent claim 1.

Regarding claims 11-13, 15-17 and 19-20, these claims are also nonobvious for at least the same reasons as given above to the extent that they encompass the same scope as claims 4-6. Withdrawal of the obviousness rejection of claims 4-6, 11-13, 15-17 and 19-20 is requested.

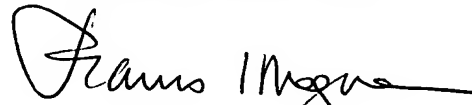
In Section 15 on page 5 of the Detailed Action, claims 7, 14, 18 and 21 have been rejected as being unpatentably obvious over *Cassagnol* in view of *Takeuchi et al* (US Patent No. 6,647,495). Claim 7 depends from independent claim 1 and is nonobvious for at least the same reasons as given above in applicant overcoming the novelty rejection of method claim 1. The same may be said for system claim 14, method claim 18 and system claim 21. Withdrawal of the obviousness rejection of claims 7, 14, 18 and 21 is requested.

The objections and rejections of the Office Action of April 23, 2008, having been obviated by amendment or shown to be inapplicable, withdrawal thereof is requested and passage of claims 1-32 to issue is solicited.

A petition for a three-month extension of time and a fee of \$1110.00 is enclosed. If the petition is missing or is for an incorrect amount or period of time, the Commissioner is authorized to deduct or credit the appropriate amount from or to our Deposit Account No. 23-0442.

Applicant also submits herewith an additional claim fee of \$416.00 for added claims 25-32. If the fee is missing or inadequate the Commissioner is authorized to deduct the fee or any shortfall from our Deposit Account No. 23-0442.

Respectfully submitted,



Francis J. Maguire
Attorney for the Applicant
Registration No. 31,391

FJM/mo
Ware, Fressola, Van Der Sluys & Adolphson LLP
755 Main Street, P.O. Box 224
Monroe, CT 06468
(203) 261-1234